2 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 681.3

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

Дмитро Янішевський
Служба безпеки України

Анотація: **Розглянуто організаційно-технічні аспекти захисту інформації в комп'ютерних системах та мережах правоохоронних органів.**
Summary: **The organizational and technical aspects of protection of the information in computer systems and networks of law-enforcement bodies are considered.**
Ключові слова: **Автоматизована система, захист інформації, засоби обчислювальної техніки, правоохоронні органи.**

I Вступ

Впровадження засобів обчислювальної техніки (ЗОТ) у діяльність правоохоронних органів набуває дедалі більшого масштабу.

Правову основу впровадження засобів обчислювальної техніки та побудованих з їх використанням автоматизованих систем становлять відповідні положення Законів України "Про Службу безпеки України", "Про міліцію", "Про оперативно-розшукову діяльність", згідно з якими зазначені системи можуть створюватись в інтересах оперативно-службової діяльності правоохоронних органів.

Разом з тим, інформація, що створюється в ході відповідної діяльності правоохоронних органів і, таким чином, висвітлює та документує її, переважним чином є інформацією з обмеженим доступом. Значну частку її віднесено до інформації, що становить державну таємницю.

Таким чином, при обробці такої інформації з використанням ЗОТ, особливо у правоохоронних органах, виникає питання щодо забезпечення потрібного режиму доступу та обробки такої інформації (відповідно, режим конфіденційності, якщо мова йде про конфіденційну інформацію, та режим секретності, якщо мова йде про інформацію, що становить державну таємницю). Іншими словами, проблему захисту інформації, що обробляється з використанням ЗОТ, з одного боку можна розглядати як вирішення питання щодо забезпечення доступу до такої інформації визначеного кола осіб, а з іншого – як необхідність забезпечення збереження такої інформації з урахуванням фізичних принципів її обробки та накопичення із застосуванням ЗОТ.

II Основна частина

Слід зауважити, що захист інформації завжди є завданням, "прив'язаним" до конкретної комп'ютерної системи. Ведучи розмову про захист інформації на рівні концепцій національної безпеки, завжди треба мати на увазі, що захищати доведеться інформацію в окремо взятій комп'ютерній системі або системах. Тому законодавче регулювання цієї проблеми, як правило, завжди матиме рамковий характер і визначатиме основи взаємовідносин у цій сфері, а конкретика (безпосередні правові приписи суб'єктам процесу захисту інформації) завжди залишатиметься прерогативою відомчого нормотворчого процесу. Тобто, можна дійти висновку, що у процесі регулювання суспільних відносин, пов'язаних з використанням "високих" (необов'язково інформаційних) технологій, завжди поставатиме проблема побудови відомчої нормативної бази як системи, що здійснює конкретизацію правових норм, закладених у нормативних актах вищого рівня, з метою безпосереднього правового регулювання. Причому, чим загальніший характер носять рамкові законодавчі акти, тим більше нормативне навантаження припадає на долю відомчих нормативно-правових актів. А недосконалість перших, взагалі ставить відомства перед проблемою самостійної розробки відповідних актів, не об'єднаних у загальнодержавному масштабі спільними концептуальними засадами.

Протягом багатьох століть проблема захисту інформації традиційно розглядалася в контексті забезпечення надійного зберігання письмових джерел (переважно паперових носіїв), охорони конфіденційних поштових повідомлень, внаслідок чого інформація фактично ототожнювалася з її носієм, що дозволяло звести завдання захисту інформації до захисту її носіїв. Поява комп'ютерної техніки змусила

переглянути основні підходи до вирішення цієї проблеми, поставила на порядок денний завдання розробки принципово нових методів унеможливлення несанкціонованого доступу до інформації, забезпечення її цілісності та доступності.

У поняття "інформація" вкладається різний зміст залежно від сфери, де воно використовується. Так, філософське трактування інформації – це все, що зменшує ступінь невизначеності нашого знання про даний предмет [4, с. 217]. У теорії зв'язку інформація – це сигнали різної фізичної природи, що передаються від їх джерела через середовище – канал зв'язку – до приймача інформації [5, с. 373]. Юридичне тлумачення інформації – це відомості про осіб, факти, події та явища, незалежно від форми їх представлення [6, с. 15].

Для дослідження проблеми захисту інформації найбільш прийнятними є її визначення через об'єкт захисту. Якщо захисту підлягає мовна інформація, то об'єктом захисту є засоби відтворення звуку і середовище його поширення. У випадку, коли захищається інформація в каналах електрозв'язку, об'єктом захисту є лінії зв'язку та апаратура перетворення (кодер/декодер). Якщо ж йдеться про комп'ютерні системи і мережі, то об'єктом захисту є машинні носії інформації, вміщена на них інформація, засоби обчислювальної техніки та канали зв'язку між комп'ютерними системами.

Якщо розглядати інформаційний процес як послідовність збору, накопичення, обробки, передачі, видачі та споживання інформації, то процес захисту інформації можна умовно поділити (за особливостями поводження з інформацією) на два етапи:

- захист інформації під час її збирання, накопичення, обробки та видачі;
- захист інформації під час споживання (також можна розглядати захист споживача в процесі споживання інформації).

На першому етапі захисту підлягає інформація на машинних носіях, технічні засоби обробки інформації та середовище її розповсюдження. Інформація у придатному для споживання вигляді, а також споживач інформації є об'єктом захисту на другому етапі.

Захист інформації можна розглядати і з точки зору захисту права власності на неї. Хоч інформація не є матеріальним об'єктом (це знання, тобто відображення дійсності, що оточує нас, у свідомості людини), вона завжди пов'язана з матеріальними носіями, якими можуть виступати мозок людини, книга, магнітна стрічка, дискета тощо. Філософське трактування інформації припускає існування останньої як абстрактної субстанції, яка існує сама по собі, але з погляду захисту інформації вона не існує без відриву від її носія. Це дає змогу поширити (з певними обмеженнями) норми майнового права на інформацію, включивши її до об'єктів права власності.

Отже, об'єкт захисту інформації має складну структуру (рис. 1), що відображає, по-перше, технологію обробки та споживання інформації, та, по-друге, її властивості як об'єкта права.

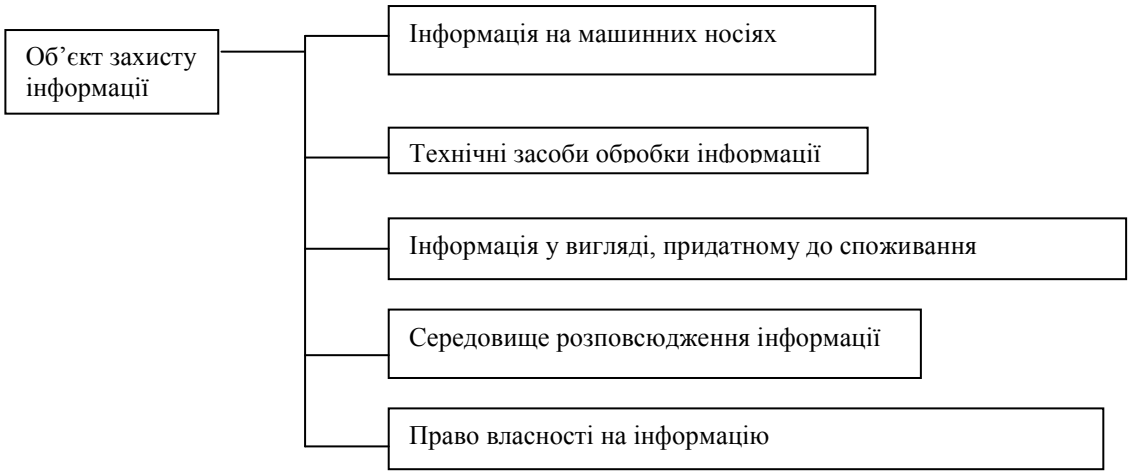

Рисунок 1 – Структура об'єкта захисту інформації

Захист інформації з точки зору об'єкта захисту можна визначити як захист самої інформації на її носіях, захист інформації в процесі її сприйняття та технічних засобів її обробки, середовища розповсюдження інформації, а також захист права власності на інформацію.

Таке визначення захисту інформації є неповним, оскільки незрозуміло, від чого потрібно її захищати. Введемо поняття загрози інформації як сукупності факторів, реалізація яких на будь-якому етапі існування інформації може призвести до небажаного впливу на неї. У процесі створення, обробки, споживання

інформації небажаний вплив на неї може проявлятися у порушенні фізичної цілісності її носіїв, несанкціонованих модифікації, отриманні та розповсюдженні, що відображає як вплив на фізичну структуру інформації та її носіїв, так і можливе порушення права власності на неї.

Визначення та оцінка загроз інформації, передумов їх виникнення та шляхів протидії їм є предметом захисту інформації (рис. 2). До предмету захисту інформації відносяться також особливості інформації, даних, носіїв даних, характеристики процесів обробки та споживання, які зумовлюють існування загроз.

Така структура об'єкта і предмета захисту інформації зумовлює різноманітність методів, що застосовуються для організації її захисту. Їхній вибір залежить від того, на яких носіях існує інформація, які технічні засоби використовуються для її обробки, в якому вигляді вона подається споживачеві

Відповідно, для захисту інформації можуть використовуватись ті ж самі методи, що й при створенні інформаційних технологій, комп'ютерних систем тощо. Це – методи системотехніки (математичне моделювання, фізичний або технічний експеримент), кібернетики (математичний експеримент, машинне моделювання, ймовірністно-статистичні методи аналізу), теоретичної інформатики (математичне моделювання, соціологічний аналіз, метод аналогій, методи пошуку оптимальних рішень), а також методи юридичних наук (методи моделювання нормативно-правової бази, методи виявлення та дослідження правовідносин, що виникають між суб'єктами інформаційних процесів).

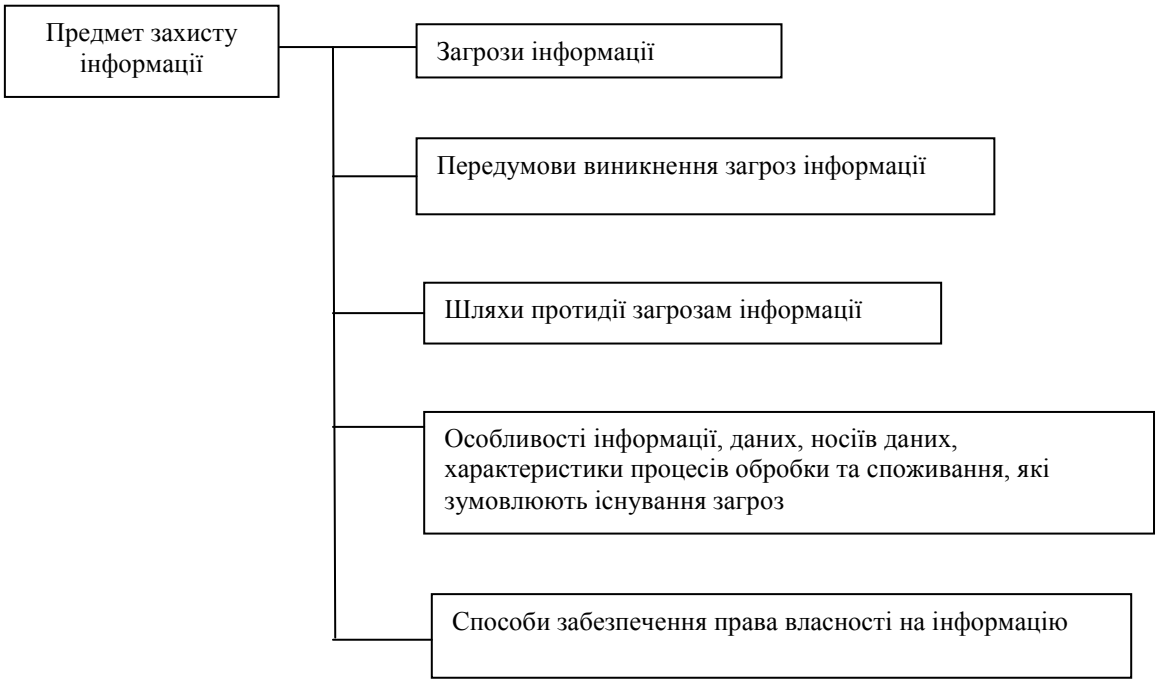

Рисунок 2 – Структура предмета захисту інформації

З урахуванням викладених вище підходів до розуміння захисту інформації, цікавим уявляється визначення шляхів організації захисту від несанкціонованого доступу в реальних умовах обробки інформації. Останні зумовлені складом апаратних та програмних засобів обробки інформації, що є найбільш поширеними на цей час.

Найбільш характерними режимами обробки інформації з використанням персональних ЕОМ (далі - ПЕОМ), на думку автора, можна визнати підготовку різного роду документів, що висвітлюють процес службової діяльності.

При цьому характерними умовами експлуатації ЗОТ (найчастіше це персональна ЕОМ автономного користування, обладнана принтером) є:

- одна персональна ЕОМ використовується кількома співробітниками;
- персональні ЕОМ експлуатуються під управлінням операційних систем сімейства Windows 9x, рідко - Windows NT/2000;
- інформація зберігається на твердому диску ПЕОМ без застосування будь-яких засобів розмежування доступу, крім організаційних (найчастіше це зберігання інформації на закріплених за користувачем зйомних

носіях даних);

- користувачі ПЕОМ мають низький рівень комп'ютерної обізнаності, що зумовлює нерозуміння ними шляхів можливого витоку інформації та несанкціонованого доступу до неї; таким чином співробітники часто можуть нехтувати вимогами щодо захисту інформації, підготовленої особисто кожним з них.

Разом з тим, необхідність виконання вимог встановленого режиму доступу до інформації, згідно з якими не припускається неконтрольований обіг та поширення інформації з обмеженим доступом, а також ознайомлення з такою інформацією осіб, які не мають до неї відношення по службі, вимагають зовсім інших підходів до принципів розмежування доступу до інформації, які мають бути реалізовані в процесі експлуатації ЗОТ.

Так, зокрема, необхідно:

- забезпечити неприпустимість вільного поширення інформації з обмеженим доступом в електронному вигляді, причому це стосується як електронних версій документів, так і проміжних їхніх копій;
- забезпечити неприпустимість ознайомлення співробітників з інформацією один одного при спільній роботі на персональній ЕОМ;
- встановити контроль за передачею електронних версій документів між співробітниками.

В [7 – 9] викладено досить багато способів вирішення цих проблем, разом з тим, серед них доцільно відзначити кілька найпростіших, але, певною мірою і найефективніших.

1) Надання кожному співробітнику можливості працювати на одній ПЕОМ таким чином, начебто для нього це дійсно персональна ЕОМ. Це можливо, щонайменш трьома шляхами:

- кожний користувач працює на закріпленому за ним зйомному НТМД, на якому знаходиться все: від операційної системи до файлів з даними; принцип простий і дешевий – попрацював, вимкнув ПЕОМ, зняв НТМД, сховав його у сейф;
- застосування операційних систем, які мають вбудовані механізми захисту, наприклад, Windows NT/2000, з використанням яких можливо так відконфігурувати робоче середовище, що кожний співробітник матиме доступ тільки до тих ресурсів ПЕОМ, до яких йому це дозволено; недолік такої схеми: у кожному підрозділі потрібен певний адміністратор, який здійснює первинне конфігурування операційної системи і, таким чином, має доступ з правами адміністратора на кожну з відконфігурованих ним систем;
- застосування зовнішніх програмно-апаратних засобів захисту інформації від НСД, комплект яких повинен бути придбаний для кожної з персональних ЕОМ; недолік: значні накладні витрати на обладнання робочих місць співробітників.

2) Впровадження локальних обчислювальних мереж і застосування механізмів розмежування доступу до інформації, вбудованих у мережеві операційні системи. При цьому можливе автоматизоване конфігурування робочого середовища користувачів (створення профілів програмного забезпечення для кожного користувача, в рамках якого визначаються усі ресурси ЛОМ і персонального комп'ютера, до яких він має доступ). Поряд з цим можливе вилучення накопичувачів на зйомних машинних носіях даних і організація ділянок роздруку документів. Тобто користувач позбавляється можливості копіювати та роздруковувати інформацію на власний розсуд.

Разом з тим, необхідно відзначити, що згідно з вимогами чинних нормативно-правових документів системи технічного захисту інформації [10] в Україні, обробка інформації з обмеженим доступом з використанням автоматизованих систем передбачає отримання дозволу на експлуатацію, тобто документу, який підтверджує відповідність вжитих заходів із захисту інформації, у тому числі й від несанкціонованого доступу, встановленим.

Постає питання щодо забезпечення виконання встановлених вимог захисту інформації і отримання такого дозволу.

На думку автора, це можливо тільки одним шляхом: впровадженням допущених до експлуатації засобів технічного та криптографічного захисту інформації. В усіх інших випадках частину вимог щодо захисту інформації перекладається на організаційні заходи, причому за відсутності згаданих вище засобів захисту на організаційні заходи покладатиметься переважна частина функцій захисту. А за умови відсутності або недостатньої чисельності кваліфікованого персоналу, який може проконтролювати реалізацію цих організаційних заходів, останні стають набором гасел, додержання яких майже ніким не виконується і про які згадують тільки у випадку витоку інформації, як про формальні правила, що були порушені.

Викладені вище умови обробки інформації, та способи захисту від несанкціонованого доступу до інформації дозволяють сформулювати певні вимоги до таких засобів захисту.

III Висновки

Засіб захисту інформації, що має використовуватись на персональній ЕОМ, на думку автора повинен бути апаратно-програмним і реалізовувати такі основні функції:

1) шифрування інформації у каталогах користувача із застосуванням апаратних засобів;

2) можливість конфігурування цих каталогів (створення захищених каталогів, призначення їх користувачам), однак конфігурування каталогів має здійснюватись тільки адміністратором;

3) ідентифікація та аутентифікація користувача з використанням щонайменш двох механізмів (як правило, це пароль та якийсь засіб ідентифікації, наприклад, електронний ключ);

4) завантаження програмного драйверу, яким встановлюються права користувачів щодо доступу до ресурсі ПЕОМ, що захищаються, до завантаження операційної системи, прозоре шифрування усієї інформації, що записується до захищених каталогів, при цьому драйвер повинен дозволяти користувачу здійснювати операції з файлами тільки у визначених каталогах;

5) контроль використання каталогів для зберігання тимчасових файлів, які утворюються при функціонуванні певних програмних засобів; у процесі роботи користувача з інформацією, що захищається, або після її завершення вміст цих каталогів повинен автоматично знищуватись.

6) система повинна контролювати експорт/імпорт інформації (у тому числі й тимчасовий через програмний буфер) із захищених каталогів в інші каталоги або її передачу каналами вводу-виводу та на інші носії даних;

7) до складу системи має входити захищений журнал фіксації певного набору дій користувачів стосовно визначених об'єктів захисту.

Зазначений перелік не претендує на всеосяжність і може уточнюватись як у бік посилення окремих вимог, так і у бік їх послаблення, разом з тим, може бути запропонований як орієнтовний при впровадженні засобів захисту інформації від несанкціонованого доступу.

Література: ***1.*** *Закон України "Про Службу безпеки України".* ***2****. Закон України "Про міліцію".* ***3.*** *Закон України "Про оперативно-розшукову діяльність".* ***4****. Философский энциклопедический словарь. – М.: "Советская энциклопедия", 1983. – 837 с.* ***5****. Шеннон К. Э. "Работы по теории информации и кибернетике". – М.: Изд-во иностр. лит-ры, 1963. – 829 с.* ***6****. Бачило И. Л., Волокитин А. В., Колчинский М. Л. и др. Федеральный закон "Об информации, информатизации и защите информации": Комментарий / РАН. Институт гос-ва и права. – М.: 1996. – 82 с.* ***7****. Голубєв В. О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів / Під заг. ред. д. ю. н. О. П. Снігерьова. – Запоріжжя.: "Павел", 1998. – 143 с.* ***8****. Медведовский И., Семьянов П., Платонов В. Атака через Internet . - С.-Пб.: НПО "Мир и семья-95", 1997. – 277 с.* ***9****. Стенг Д, Мун С. Секреты безопасности сетей. – К.: Диалектика, 1996. – 543 с.* ***10****. "Положення про технічний захист інформації в Україні", затверджене Указом Президента України від 27. 09. 99 р. № 1229/99 // Безопасность информации. –- 2000. - № 1. – С. 73 – 75.*

УДК 621.391:519.2

АСИМПТОТИЧЕСКИЕ СООТНОШЕНИЯ ДЛЯ ВЕРОЯТНОСТЕЙ ЧИСЛА НЕСКОМПРОМЕТИРОВАННЫХ КЛЮЧЕЙ В СХЕМАХ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ПОСТРОЕННЫХ НА ОСНОВЕ БЛОЧНЫХ КОДОВ

Антон Алексейчук, Сергей Конюшок
СФ СБ Украины в составе ВИТИ НТУУ "КПИ"

Аннотация: **Рассматривается вероятностная модель процесса компрометаций корреспондентов в определенных схемах широковещательного распределения ключей, построенных на основе ортогональных таблиц силы 1 или 2. Получены точные оценки биномиальных моментов и асимптотические выражения вероятностей числа нескомпрометированных ключей в этих схемах после компрометации случайного равновероятного *t*-подмножества корреспондентов.**

Summary: **It is considered the probabilistic model of the correspondents compromising process in some broadcast key distribution schemes, built on base of orthogonal arrays of strength 1 or 2. As a result, we obtain proper bounds for binomial moments and asymptotic expressions of probability of the number non-compromising keys in these schemes under condition of random equiprobable t- subset correspondents compromising.**

Ключевые слова: **Схема распределения ключей, компрометация корреспондентов, ортогональная таблица, распределение Пуассона.**